THIS CORRESPONDENCE IS SENT TO YOU AS ORGANIZATIONAL ELECTRONIC MAIL IAW THE PROVISIONS OF AR 25-11, RECORD COMMUNICATIONS AND THE PRIVACY COMMUNICATIONS SYSTEM, AND AMCR 25-1, ELECTRONIC MAIL. THIS IS THE OFFICIAL COPY. YOU WILL NOT RECEIVE A PAPER COPY.

AMCIO-A (380-19a) 13 Mar 2002

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Interim Policy Guidance to AMC Supplement 1 to AR 380-19, Systems Security, U.S. Army Materiel Command (AMC) on Computer Security Incident Reporting

1. References:

a. Army Regulation (AR) 380-19, Information Systems Security, 27 February 1998.

b. AMC Supplement 1 to AR 380-19, Information Systems Security, 1 December 2000.

c. Memorandum, AMCIO-F, Subject: AMC Incident Reporting Procedures for Year 2000 (Y2K), 13 December 1999.

2. Purpose: This policy rescinds AMCIO-F Memorandum dated December 13, 1999 and
will be incorporated into the next update of reference 1b. This policy is critical to AMC and immediately defines a formal after action reporting process to ensure AMC responds promptly and effectively to computer security incidents within this Command.

3. As noted in Army Regulation (AR) 380-19, Information Systems Security, 27 February 1998 and AMC Supplement to AR 380-19, Information Systems Security, 1 December 2000 all Army organizations and activities must:

a. Report all computer security incidents and intrusions using the Army Computer Emergency Response Team (ACERT) “Intrusion Checklist”. A template of this checklist can be found on the ACERT website: <https://www.acert.belvoir.army.mil/avrf/compromised_form.htm>. A copy of the current template is included at enclosure 1.

b. Submit these reports according to the procedures outlined in Paragraph 2-27 of AR 380-19.

4. In addition, AMC organizations and activities must comply with the following:

a. All AMC computer security incidents reportable to ACERT will also be reported to the AMC Information Assurance Program Manager (IAPM), the ARL Center for Intrusion Monitoring and Protection (CIMP), and a copy furnished to the major subordinate commands (MSCs) and local IAMs. Reports should be e-mailed to amcio-iapm@hqamc.army.mil and arlcert@arl.army.mil, as well as coordinated with the local IAMs and installation command staff, as required by MSC/installation policies.

b. The HQ AMC Emergency Operations Center (EOC) recently issued new direction from the Commanding General on reporting of intrusions at AMC facilities. Copies of this procedure are provided for your information and appropriate action (ENCLOSURE 2). All intrusion reports provided through the EOC channels must be sent via SIPRNET.

c. If an incident is categorized either as Root Level Compromise (Category 1); User Level Compromise (Category 2); Poor Security Practice (Category 5); Malicious Code (Category 7) and is directed by either ACERT or HQ AMC also submit within five days, via e-mail, an After Action Report (AAR) to the AMC Chief of Staff (amccs@hqamc.army.mil) and a copy furnished to the AMC IAPM (amcio-iapm@hqamc.army.mil <mailto:amcio-iapm@hqamc.army.mil>). See enclosure 3 for the AAR format and Enclosure 4 for incident reporting categories.

d. AMC major subordinate commands, installations, or activities may submit written reclamas to the AMC IAPM (amcio-iapm@hqamc.army.mil <mailto:amcio-iapm@hqamc.army.mil>) to explain any disagreements with the assignment of responsibility and/or the categorization of a reportable computer security incident as defined in this policy. Courtesy copies should be provided to the ARL CIMP (arlcert@arl.army.mil). Written reclamas must:

(1) Not delay or otherwise obstruct any required actions that must be taken to resolve the reported computer security incident.

(2) Be submitted as promptly as possible preferably within 24 hours of incident reporting for Category 1 and 2 computer security incidents, and within 48 hours of incident reporting for Category 5 and 7 computer security incidents.

e. Fulfill as a minimum, the incident reporting responsibilities outlined at


encl-1_031502.doc


encl-2031502.doc


encl-3_031502.doc


encl-4_031502.doc


encl-5_031502.doc

sure 5.

5. Point of contact for this is Mr. Gary Black, DSN 767-4015, commercial (703) 617-4015 or e-mail: BlackG@hqamc.army.mil <mailto:BlackG@hqamc.army.mil>.

FOR THE COMMANDER:

//signed//
5 Encls JAMES D. BUCKNER
as Chief Information Officer

DISTRIBUTION:
AMC CIOs
AMC DOIMS
AMC-IA-INST
AMC-IA-MSC
AMC SRAS